IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of: **Pasi ERONEN**	:	Confirmation No.: **8800**
Serial No: **10/751,300**	:	Examiner: **Canh LE**
Filed: **January 2, 2004**	:	Group Art Unit: **2139**

For: **REPLAY PREVENTION MECHANISM FOR EAP SIM AUTHENTICATION**

Mail Stop Appeal Briefs-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANTS (37 CFR §41.37)

Sir:

This Appeal Brief is in furtherance of the Notice of Appeal filed January 2, 2008. The Notice of Appeal was filed in response to the final Office Action of October 4, 2007.

I hereby certify that this paper is being deposited with the U.S. Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Briefs-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Jennifer Hanlon — Feb. 26, 2008

Jennifer Hanlon — Date

Table of Contents

I. REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is Nokia Corporation, a corporation organized under the laws of Finland.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

There are no related appeals or interferences.

III. STATUS OF CLAIMS (37 C.F.R. § 41.37(c)(1)(iii))

Claims 1-11 are pending in the application. Claims 1-11 are rejected. Claim 5 is objected to. The rejections of claims 1-11 are appealed.

IV. STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

All amendments filed have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

The independent claims are 1, 6 and 8. Independent claim 1 recites a method for use by a telecommunications terminal (*e.g.* telecommunications terminal 10 of Fig. 1) in authenticating the telecommunications terminal. (*See* specification page 5, line 28 through page 6, line 12). The method comprises encoding random numbers previously used for authenticating the telecommunications terminal, so as to provide a data structure (*e.g.* data structure 21 of Fig. 2) consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers. (*See* specification page 8, lines 3-29, *see also* Fig. 2). The method further comprises checking the data structure to determine whether a candidate random number is not one of the previously used random numbers, wherein the data structure is such as to at least provide a true answer as to whether the candidate random number is not one of the

previously used random numbers. (*See* specification page 3, lines 9-27, and page 6, line 20 through page 7, line 8).

Independent claim 6 recites an apparatus for use by a telecommunication terminal (*e.g.* telecommunications terminal 10 of Fig. 1) in authenticating the telecommunications terminal to an access network. (*See* specification page 5, line 28 through page 6, line 12). The apparatus comprises means (*e.g.* MWLAN module 11, MGSM module 12, and authenticator module 14 of Fig. 1) for encoding random numbers previously used for authenticating the telecommunications terminal, so as to provide a data structure (*e.g.* data structure 21 of Fig. 2) consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers. (*See* specification page 8, lines 3-29, *see also* Fig. 2). The apparatus further comprises means (*e.g.* MWLAN module 11, MGSM module 12, and authenticator module 14 of Fig. 1) for checking the data structure to determine whether a candidate random number is not one of the previously used random numbers, wherein the data structure is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers. (*See* specification page 4, line 18 through page 5, line 4, and page 6, line 20 through page 7, line 8).

Independent claim 8 recites an apparatus for use by a telecommunication terminal (*e.g.* telecommunications terminal 10 of Fig. 1) in authenticating the telecommunications terminal to an access network. (*See* specification page 5, line 28 through page 6, line 12). The apparatus comprises an authenticator module (*e.g.* authenticator module 14 of Fig. 1) and one or more Bloom filter modules (*e.g.* MWLAN module 11, MGSM module 12 of Fig. 1), configured to encode random numbers previously used for authenticating the telecommunications terminal, so as to provide a data structure (*e.g.* data structure 21 of Fig. 2) consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used

random numbers. (*See* specification page 7, line 17 through page 8, line 29, and page 13, lines 13-33; *see also* Fig. 2, Fig. 3). The authenticator module and one or more Bloom filter modules, further configured to check the data structure to determine whether a candidate random number is not one of the previously used random numbers, wherein the data structure is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers. (*See* specification page 6, line 20 through page 7, line 8, and page 8, line 3 through page 10, line 13).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Claims 1-3 and 5-10 are rejected under 35 U.S.C. §103(a) as being unpatentable over Patel ("Analysis of EAP-SIM Session Key Agreement", IETF EAP mailing, May 29, 2003, pp. 1-4) in view of Dharmapurikar et al. ("Longest Prefix Matching Using Bloom Filter", SIGCOMM'03, August 25-29, 2003, pp. 201-212). Claims 4 and 11 are rejected under 35 U.S.C. §103(a) as being unpatentable over Patel ("Analysis of EAP-SIM Session Key Agreement", IETF EAP mailing, May 29, 2003, pp. 1-4) in view of Dharmapurikar et al. ("Longest Prefix Matching Using Bloom Filter", SIGCOMM'03, August 25-29, 2003, pp. 201-212) and further in view of Aguilera et al. (US Patent Application Publication US 2005/002209).

VII. ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

Rejections under 35 U.S.C. § 103(a) as unpatentable over Patel in view of Dharmapurikar et al

Claim 1

With regard to claim 1, the present invention provides a solution to various GSM EAP/SIM authentication problems, and in particular, provides a method for determining whether

a candidate RAND[1] included in a RAND challenge (in e.g. an EAP/SIM authentication message exchange) is *not* one of one or more previously used RANDs. Claim 1 recites a method including a step of encoding the (one or more) previously used RANDs using a data structure consisting of an ordered set of components all having a starting value of zero, but the value for a component may be set to one based on the previously used RANDs. (*See* specification page 8, lines 3-29, *see also* Fig. 2). The data structure is then checked to determine whether the candidate RAND is *not* one of the previously used RANDs. (*See* specification page 6, line 20 through page 7, line 8). Importantly, all of the bits of each previously used RAND are used in determining whether to set the value of a component to one. More specifically, each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set of components, the component is pointed to by any of a plurality of pointer values (i.e. the pointer value is a number that indicates the position of the component in the ordered set) each based on *all the bits* of a respective one of the previously used RANDs. (*See* specification page 3, lines 9-27, and page 8, line 3 through page 10, line 13). Figure 2 is helpful to an understanding of this encoding.

One embodiment of the data structure is based on a so-called Bloom filter. Claim 2 encompasses such an embodiment. From Wikipedia:

> The Bloom filter, conceived by Burton H. Bloom in 1970, is a space-efficient probabilistic data structure that is used to test whether or not an element is a member of a set. False positives are possible, but false negatives are not. Elements can be added to the set, but not removed (though this can be addressed with a counting filter). The more elements that are added to the set, the larger the probability of false positives.

The Office concedes that the primary reference Patel does not disclose the recited encoding of previously used RANDs to provide a data structure and the recited checking of the data structure to determine whether a candidate RAND is not one of the previously used RANDs. For such disclosure, the Office relies on Dharmapurikar, which provides an algorithm for IP routing lookup based on Bloom filter theory. The Office thus asserts that it would have been

---

[1] A RAND, as illustrated in the application, is e.g. a 128-bit random number used with a root key K_i (up to 128 bits) to generate a 64-bit key K_c and a 32-bit value SRES included in a RAND challenge.

obvious at the time of the invention, for one of skill in the art to modify the teachings of Patel according to the teachings of Dharmapurikar, so as to arrive at the invention.

In fact, though, Patel *teaches away* from the invention. At section 2.2.1, Patel teaches that:

> There is actually *no solution to this problem* [of providing for session independence] as long as one is working with GSM triplets as the fundamental source of keying. The above solutions to strengthen the 64 bit [*sic*] to 128 bits are of no use in creating session independence, and it's hard to see how one could do it easily.
>
> One approach possible but *not practical* is for the client *to store all the past RAND vectors* its [*sic*] seen and to make rue that they are not repeated. ...
>
> Since its [*sic*] not practical to store all past values, perhaps the client can *store the most recent n RAND values* and make sure they are not repeated. This may *give some practical protection* in practice. Actually the whole RAND vector doesn't need to be stored, *just a part of the RAND*, for example 32 bits *can be stored* and looked for repeats [*sic*]; ... .

So the most that can be learned from Patel is that one should store only part of the most recent n RAND values, and then look for repeats. *In direct contrast*, the invention requires determining a data structure of components (*e.g.* data structure 21 of Fig. 2) each having a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set of components, the component is pointed to by any of a plurality of pointer values (i.e. the pointer value is a number that indicates the position of the component in the ordered set) each based on *all the bits* of a respective one of previously used RANDs. (*See* specification page 3, lines 9-27, and page 8, line 3 through page 10, line 13; *see also* Fig. 2, Fig. 3). On the contrary, the best Patel could suggest is that *only some of the bits* be used in looking for repeats (because of memory limitations).

Now per the MPEP at 2143.01 (VI), a proposed modification cannot change the principle of operation of a reference:

> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959) (Claims were directed to an oil seal comprising a bore engaging portion with outwardly biased resilient spring fingers inserted in a resilient sealing member. The primary reference relied upon in a rejection based on a combination of references disclosed an oil seal wherein the bore engaging portion was reinforced by a cylindrical sheet metal casing. Patentee taught the device required rigidity for operation,

> whereas the claimed invention required resiliency. The court reversed the rejection holding the "suggested combination of references would require a substantial reconstruction and redesign of the elements shown in [the primary reference] as well as a change in the basic principle under which the [primary reference] construction was designed to operate." 270 F.2d at 813, 123 USPQ at 352.).

Appellant therefore respectfully submits that altering the teachings of Patel according to the teachings of Dharmapurikar (and so arriving at the use of a Bloom filter) is not obvious.

Further, although Dharmapurikar provides a general description of Bloom filter theory and an algorithm for *IP routing lookup* based on Bloom filter theory, *Dharmapurikar does not suggest using a Bloom filter in a RAND challenge.* Thus, Dharmapurikar does not teach or suggest either the encoding or the checking steps recited in claim 1, so that even the combination fails to teach or suggest these steps. In other words, the teachings of Dharmapurikar are limited to applications of Bloom filter theory to IP routing lookup. Further, Dharmapurikar is only interested in finding a match,[2] not determining that there is *not* a match, as required by claim 1. Thus, there is no suggestion in either Dharmapurikar or Patel of applying Bloom filter theory to guarding against repeats in a RAND challenge. Appellant therefore respectfully submits that the invention as in claim 1 is thus patentable over the combination of Patel and Dharmapurikar, because per the MPEP at 2143.03:

> To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

For at least these reasons, claim 1 is believed patentable over Patel in view of Dharmapurikar. Appellant therefore respectfully requests the rejection of claim 1 be reversed and withdrawn by the Board.

---

[2] At page 201, right-hand column, Dharmapurikar explains that the problem being solved is "to search variable-length address prefixes in order to find the longest matching prefix of an I destination address [for each packet traversing a router] and retrieve the corresponding forwarding information."

Claim 2

Claim 2 depends from independent claim 1 and recites additional required features not recited in claim 1, and therefore is patentable over of the cited references, at least in view of its dependency.

Claim 3

Claim 3 depends from independent claim 1 and recites additional required features not recited in claim 1, and therefore is patentable over of the cited references, at least in view of its dependency.

Claim 4

Claim 4 depends from independent claim 1 and recites additional required features not recited in claim 1, and therefore is patentable over of the cited references, at least in view of its dependency.

Claim 5

Claim 5 is a computer program product claim for performing the method of independent claim 1, and is rejected for the same reasons as claim 1. Therefore, for at least the reasons discussed above in relation to claim 1, claim 5 is patentable over of the cited references.

Claim 6

Independent claim 6 is an apparatus claim comprising means for performing the method of independent claim 1, and is rejected for the same reasons as claim 1. Therefore, for at least the reasons discussed above in relation to claim 1, independent claim 6 is patentable over of the cited references.

Claim 7

Claim 7 is a system claim including an apparatus as in independent claim 6, which in turn comprises means for performing the method of independent claim 1, and is rejected for the same reasons as claim 1. Therefore, for at least the reasons discussed above in relation to claim 1, claim 7 is patentable over of the cited references.

Claim 8

Independent claim 8 is an apparatus claim containing limitations similar to those recited in claim 1, and is rejected for the same reasons as claim 1. Therefore, for at least the reasons discussed above in relation to claim 1, claim 8 is patentable over of the cited references.

Claim 9

Claim 9 depends from independent claim 8 and recites additional required features not recited in claim 8, and therefore is patentable over of the cited references, at least in view of its dependency.

Claim 10

Claim 10 depends from independent claim 8 and recites additional required features not recited in claim 8, and therefore is patentable over of the cited references, at least in view of its dependency.

Claim 11

Claim 11 depends from independent claim 8 and recites additional required features not recited in claim 8, and therefore is patentable over of the cited references, at least in view of its dependency.

Conclusion

For the reasons discussed above, Appellant respectfully submits that the rejections of the Office Action have been shown to be inapplicable, and respectfully requests that the Board reverse the rejections of pending claims 1-11.

Per 37 CFR § 41.31, a check in the amount of $510 is enclosed. If any additional fee is required for submission of this Appeal Brief, the Commissioner is hereby authorized to charge Deposit Account No. 23-0442.

Respectfully submitted,

Date: 2-26-08

Cathy A. Sturmer
Agent for the Appellant
Registration No. 60,869

CAS/cas

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676

USPTO Customer No. 004955

VIII. CLAIMS APPENDIX

The claims involved in the appeal are as follows:

1. A method for use by a telecommunications terminal (10) in authenticating the telecommunications terminal (10), comprising:

encoding random numbers previously used for authenticating the telecommunications terminal (10), so as to provide a data structure (21) consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers; and

checking the data structure (21) to determine whether a candidate random number is not one of the previously used random numbers;

wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers.

2. A method as in claim 1, wherein in encoding the previously used random numbers, a set of hash functions is used each providing a value in a range equal to the number of components of the data structure (21), and for each previously used random number, each of the hash functions is evaluated and the component in the ordered set of components at the position indicated by the hash function value is set to one.

3. A method as in claim 1, wherein in encoding the previously used random numbers, the previously used random numbers are used as the pointer values.

4. A method as in claim 1, wherein the data structure (21) is a multi-part data structure (21) with each part having an upper limit on the number of random number values it can indicate as one of the previously used random number values, wherein each part has values based on only some of the previously used random numbers, and wherein all most recently received random numbers are used in determining component values in only one of the parts, and further wherein

when an upper limit is reached for the one of the parts, another of the parts is reset.

5. A computer program product comprising:

a computer readable storage structure embodying computer program code thereon for execution by a computer processor in a terminal (10),

wherein said computer program code includes instructions for performing the method of claim 1.

6. An apparatus for use by a telecommunication terminal (10) in authenticating the telecommunications terminal (10) to an access network, comprising:

means (11 12 14) for encoding random numbers previously used for authenticating the telecommunications terminal (10), so as to provide a data structure (21) consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers; and

means (11 12 14) for checking the data structure (21) to determine whether a candidate random number is not one of the previously used random numbers;

wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers.

7. A system, comprising:

a telecommunication terminal (10), and

a radio access network configured for cellular communication with the telecommunication terminal (10),

wherein the telecommunication terminal (10) includes an apparatus as in claim 6.

8. An apparatus for use by a telecommunication terminal (10) in authenticating the telecommunications terminal (10) to an access network, comprising an authenticator module (14) and one or more Bloom filter modules (11 12), configured to:

encode random numbers previously used for authenticating the telecommunications terminal (10), so as to provide a data structure (21) consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers; and

check the data structure (21) to determine whether a candidate random number is not one of the previously used random numbers;

wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers.

9. An apparatus as in claim 8, wherein for encoding the previously used random numbers the authenticator module (14) and one or more Bloom filter modules (11 12) are configured so that a set of hash functions is used each having a range equal to the number of components of the data structure (21), and for each previously used random number, each of the hash functions is evaluated and the component in the ordered set of components at the position indicated by the hash function value is set to one.

10. An apparatus as in claim 8, wherein the previously used random numbers are the pointer values.

11. An apparatus as in claim 8, wherein the data structure (21) is a multi-part data structure (21) with each part having an upper limit on the number of random number values it can indicate as one of the previously used random number values, wherein each part has values based on only some of the previously used random numbers, and wherein all most recently received random numbers are used in determining component values in only one of the parts, and further wherein for encoding the previously used random numbers the authenticator module (14) and one or more Bloom filter modules (11 12) are configured so that when an upper limit is reached for the one of the parts, another of the parts is reset.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.